Dena C. Sharp (SBN 245869)
dsharp@girardsharp.com
Adam E. Polk (SBN 273000)
apolk@girardsharp.com
Simon S. Grille (SBN 294914)
sgrille@girardsharp.com
Isabel Velez (SBN 359574)
ivelez@girardsharp.com
GIRARD SHARP LLP
601 California Street, Suite 1400
San Francisco, CA 94108
Telephone: (415) 981-4800
Facsimile: (415) 981-4846

Attorneys for Plaintiff and the Putative Class

UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF CALIFORNIA (Oakland Division)

ASHLEY JOHNSON on behalf of herself and all others similarly situated,

Plaintiff,

v.

CALIFORNIA PHYSICIANS' SERVICE D/B/A BLUE SHIELD OF CALIFORNIA,

Defendant.

Case No.

CLASS ACTION COMPLAINT FOR:

1. VIOLATIONS OF CAL. PENAL CODE § 631, *et seq*.;
2. VIOLATIONS OF CAL. PENAL CODE § 638.51(a);
3. VIOLATIONS OF CAL. CIV. CODE § 56, *et seq*.;
4. VIOLATIONS OF CAL. BUS. & PROF. CODE § 17200, *et seq.*;
5. VIOLATIONS OF CAL. CONST. ART. 1 § 1;
6. VIOLATION OF THE ELECTRONIC PRIVACY ACT, 18 U.S.C. § 2510, *et seq.*
7. INTRUSION UPON SECLUSION;
8. PUBLICATION OF PRIVATE FACTS; AND
9. BREACH OF CONFIDENCE.

JURY TRIAL DEMANDED

Plaintiff Ashley Johnson ("Plaintiff") brings this class action complaint ("Complaint") on behalf of herself and all others similarly situated (the "Class Members") against California Physicians' Service d/b/a/ Blue Shield of California ("Blue Shield," "BSCA" or "Defendant"), one of the largest health care insurers in California. Blue Shield partners with doctors and practice groups to provide medical coverage including HMOs, PPOs, Dental care, and Vision Care, and operates, controls, and manages over 380 hospitals state wide, working with over 75,000 physicians. Defendant owns and controls blueshieldca.com and related webpages (the "Website"), and it also owns and controls a mobile app (the "App") (collectively the "Web Properties").

NATURE OF THE ACTION

1. Plaintiff brings this class action lawsuit to address BSCA's disclosure of its patients confidential personally identifiable information ("PII") and protected health information ("PHI") (collectively referred to as "Private Information") to unauthorized third parties, including Google LLC ("Google").

2. BSCA's unauthorized disclosures of Private Information occurred because of its use of tracking technologies that BSCA installed on its Web Properties, including but not limited to the Google Analytics tool, Google Ads tool, and other related tracking tools (collectively, "Tracking Technologies" or "Tracking Tools").

3. The Tracking Technologies allow unauthorized third parties to intercept the contents of patients' communications, receive and view patients' Private Information, mine it for purposes unrelated to the provision of healthcare, and monetize it by using it to deliver targeted advertisements to specific individuals.

4. BSCA owns and controls the Web Properties, which it makes available to Plaintiff and other patients to use for the following:

- *Manage Healthcare*: Members can access information about doctors, specialists, and hospitals within BSCA's PPO, HMO, dental, and vision networks. The Web Properties also facilitate telehealth appointments and provide resources for mental health care.

- *File Insurance Claims*: The Web Properties support claim management, enabling members to file claims online and track their status.
- *Pay Bills*: Insured individuals can pay their premiums directly through the Web Properties using secure payment options.
- *Access Plan Information*: Members can review details about their health plans, including coverage options for Medi-Cal, Medicare, and other insurance plans.
- *Resource Navigation*: The Web Properties offer tools to find urgent care facilities, compare costs for different services, and prepare for non-emergency medical needs.

5. In doing so, and by designing its Web Properties in the manner described throughout this complaint, BSCA knew or should have known that its patients would use the Web Properties to communicate Private Information in conjunction with obtaining and receiving medical services and insurance from BSCA.

6. Plaintiff and other Class Members who used BSCA's Web Properties reasonably believed they were communicating only with their trusted healthcare and insurance providers, and nothing about the Web Properties' appearance indicated that unauthorized third parties such as Google would intercept and obtain Private Information submitted by patients.

7. Unbeknownst to Plaintiff and Class Members, however, the Tracking Technologies embedded on BSCA's Web Properties contain source code that surreptitiously track, record, and disseminate Plaintiff's and Class Members' online activity and communications (including Private Information) to Google without first obtaining permission, in violation of HIPAA, state laws, industry standards, and patient expectations.

8. By installing and using Tracking Technologies on its Web Properties, BSCA effectively planted a bug on Plaintiff's and Class Members' web browsers and devices, which caused their communications to be intercepted, accessed, viewed, and captured by third parties in real time, as they were communicated by patients, based on BSCA's chosen parameters.

9. For example, BSCA used Google Analytics and related tools that communicate with Google Ad Services and DoubleClick to track users actions and communications on the Web

Properties. Operating as designed and as implemented by BSCA, Google Analytics and other Tracking Tools caused Plaintiff's and Class Members' Private Information to be unlawfully intercepted and surreptitiously disclosed to third parties.

10. On April 9, 2025, BSCA issued a Notice of Data Breach to insurance plan participants which stated in part the following:[1]

> Blue Shield of California has begun notifying certain members of a potential data breach that may have included elements of their protected health information.
>
> ***
>
> **What happened**
>
> Like other health plans, Blue Shield historically used the third-party vendor service, Google Analytics, to internally track website usage of members who entered certain Blue Shield sites. We were doing this to improve the services we provide to our members.
>
> On February 11, 2025, Blue Shield discovered that, between April 2021 and January 2024, Google Analytics was configured in a way that allowed certain member data to be shared with Google's advertising product, Google Ads, that likely included protected health information. Google may have used this data to conduct focused ad campaigns back to those individual members. We want to reassure our members that no bad actor was involved, and, to our knowledge, Google has not used the information for any purpose other than these ads or shared the protected information with anyone.
>
> Blue Shield severed the connection between Google Analytics and Google Ads on its websites in January 2024. We have no reason to believe that any member data has been shared from Blue Shield's websites with Google after the connection was severed. Upon discovering the issue, Blue Shield immediately initiated a review of its websites and security protocols to ensure that no other analytics tracking software is impermissibly sharing members' protected health information.
>
> **What information was involved**
>
> The information that may have been impacted includes the following:
>
> Insurance plan name, type and group number; city; zip code; gender; family size; Blue Shield assigned identifiers for members' online accounts; medical claim service date and service provider, patient name, and patient financial responsibility; and "Find a Doctor" search criteria and results (location, plan name and type, provider name and type).

[1] *See* https://news.blueshieldca.com/notice-of-data-breach (last visited April 9, 2025).

11. In the Notice of Data Breach, Blue Shield admits, among other things:

(a) BSCA ***voluntarily*** shared information with Google. While characterized as a "data breach," no hacker or "bad actor" obtained unauthorized access to BSCA's Web Properties. The purported "data breach" is referred to herein as the "Data Disclosure."

(b) The Data Disclosure "likely included protected health information" or PHI such as "medical claim service date and service provider, patient name, and patient financial responsibility; and "Find a Doctor" search criteria and results (location, plan name and type, provider name and type)."

(c) Google used this Private Information to conduct focused ad campaigns back to those individual members.

(d) Despite the fact that BSCA "severed the connection between Google Analytics and Google Ads on its websites in January 2024," BSCA claims to have not discovered its disclosure of PHI to Google until February of 2025. And it did not send notification to affected persons until April, 2025.

12. The Office for Civil Rights at HHS has issued a Bulletin to highlight the obligations of HIPAA covered entities and business associates ("regulated entities") under the HIPAA Privacy, Security, and Breach Notification Rules ("HIPAA Rules") when using online tracking technologies.[2] The Bulletin expressly provides (in bold type) that "**[r]egulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules.**" In other words, HHS has expressly stated that BSCA's implementation of the Tracking Technologies violates HIPAA Rules.

13. The information BSCA divulged to unauthorized third parties such as Google allowed those entities to learn that specific individuals were patients seeking and receiving treatment with providers covered by BSCA's insurance plan, and that they were seeking to submit

[2] *See Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, U.S. DEPT. OF HEALTH & HUMAN SERV., https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.

claims, pay bills, and receive other health care related services. In turn, this information was used and/or sold to additional unauthorized parties for use in marketing and geotargeting.

14. Patients do not anticipate that their trusted healthcare and insurance provider will send their Private Information to social media and marketing companies for future exploitation and targeted marketing.

15. Neither Plaintiff nor any other Class Member signed a written authorization permitting BSCA to send their Private Information to Google.

16. Similarly, BSCA does not have a HIPAA-compliant Business Associate Agreement in place with Google.

17. In response to the use of Tracking Technologies by HIPAA covered entities, like BSCA, the recently issued HHS Bulletin warns that:

> An impermissible disclosure of an individual's PHI not only violates the Privacy Rule but also may result in a wide range of additional harms to the individual or others. For example, an impermissible disclosure of PHI may result in identity theft, financial loss, discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others identified in the individual's PHI. Such disclosures can reveal incredibly sensitive information about an individual, including diagnoses, frequency of visits to a therapist or other health care professionals, and where an individual seeks medical treatment. While it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors, because of the proliferation of tracking technologies collecting sensitive information, now more than ever, it is critical for regulated entities to ensure that they disclose PHI **only** as expressly permitted or required by the HIPAA Privacy Rule. [3]

18. Courts have repeatedly recognized the importance of online privacy, particularly as it relates to health information.

19. Consequently, Plaintiff brings this action to address and rectify the illegal conduct and actions described herein, to enjoin BSCA from making similar disclosures of its patients'

[3] *Id.*

Private Information in the future, and to require BSCA to fully articulate, *inter alia*, the specific Private Information disclosed to third parties and to identify all the recipients of that information.

20. As a result of BSCA's conduct, Plaintiff and Class Members have suffered numerous injuries, including invasion of privacy, loss of benefit of the bargain, diminution of value of the Private Information, statutory damages, and the continued and ongoing risk to their Private Information.

21. Plaintiff seeks to remedy these harms and bring causes of action for (1) violations of Cal. Penal Code § 631, *et seq*.; (2) violations of Cal. Civ. Code § 56, *et seq*.; (3) violations of Cal. Bus. & Prof. Code § 17200, *et seq*.; (4) violations of Cal. Const. Art. 1 § 1; (5) violation of the Electronic Communications Privacy Act 18 U.S.C. § 2510, *et seq*.; (6) intrusion upon seclusion; (7) publication of private facts; and (8) breach of confidence.

JURISDICTION AND VENUE

22. This Court has subject matter jurisdiction under 28 U.S.C. § 1332(d) (the Class Action Fairness Act) because the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and a member of the Class is a citizen of a different state than BSCA. This Court also has subject matter jurisdiction under 28 U.S.C. § 1331 because this action arises under 18 U.S.C. § 2510, et seq. (the Electronic Communications Privacy Act).

23. This Court has supplemental jurisdiction over the state law claims under 28 U.S.C. § 1367 because the state law claims form part of the same case or controversy under Article III of the United States Constitution.

24. This Court has personal jurisdiction over Defendant because its corporate headquarters is located in this District.

25. Venue is proper in this District because a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

DIVISIONAL ASSIGNMENT

26. Pursuant to L.R. 3-2(c), assignment to this division is proper because a substantial part of the conduct which gives rise to Plaintiff's claims occurred in this District.

THE PARTIES

27. Plaintiff Ashley Johnson is a citizen and resident of the State of California and is domiciled in Los Angeles, California.

28. California Physicians' Service d/b/a Blue Shield of California is a mutual benefit corporation and health plan, founded in 1939 by the California Medical Association. It is headquartered in Oakland, California, and serves 4.5 million health plan members and more than 77,000 physicians across the state.

FACTUAL ALLEGATIONS

A. Background

i. Background of California Invasion of Privacy Act

29. The California Legislature enacted the California Invasion of Privacy Act ("CIPA") to protect the privacy rights of California citizens. In doing so, the California Legislature expressly recognized that "the development of new devices and techniques for the purpose of eavesdropping upon private communications … has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society." Cal. Penal Code § 630.

30. CIPA prohibits aiding or permitting another person to willfully—and without the consent of all parties to a communication—read or learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from or received at any place within California.

31. To establish liability under CIPA, Plaintiff need only establish that BSCA does, or did, any of the following:

> Intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system; or
>
> Willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads or attempts to read or learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line or cable or is being sent from or received at any place within this state; or

> Uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or
>
> Aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section.

32. Violations of CIPA are not limited to phone lines but also apply to "new technologies" such as computers, the Internet, and email.[4]

33. CIPA affords a private right of action to any person who has been subjected to a violation of the statute to seek injunctive relief and statutory damages of $5,000 per violation, regardless as to whether they suffered actual damages. Cal. Penal Code § 637.2(a)(1).

34. Moreover, CIPA § 638.51(a) proscribes any "person" from "install[ing] or us[ing] a pen register or a trap and trace device without first obtaining a court order."

35. A "pen register" is a "device or process that records or decodes dialing, rerouting, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication." Cal. Penal Code § 638.50(b).

36. By contrast, a "trap and trace device" is a "device or process that captures the incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing, or signaling information reasonably likely to identify the source of a wire or electronic communication, but not the contents of a communication." *Id.*

37. A "pen register" is a "device or process" that records outgoing information, whereas a "trap and trace device" is a "device or process" that recording incoming information.

38. Although CIPA was enacted before the creation of the Tracking Technologies discussed in this Complaint, "the California Supreme Court regularly reads statutes to apply to new technologies where such a reading would not conflict with the statutory scheme." *In re Google Inc*. 2013 WL 5423918, at *21 (N.D. Cal. Sep. 26, 2013).

---

[4] *See In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589 (9th Cir. 2020) (reversing dismissal of CIPA and common law privacy claims based on Facebook's collection of consumers' internet browsing history).

39. Individuals may bring an action against the violator of any provision of CIPA, including § 638.51, for $5,000 per violation. Cal. Penal Code § 637.2(a)(1).

ii. *Background of the Confidentiality of Medical Information Act*

40. Pursuant to the California Confidentiality of Medical Information Act ("CMIA"), "A provider of health care . . . shall not disclose medical information regarding a patient of the provider of health care . . . without first obtaining an authorization, except as provided in subdivision (b) or (c)." § 56.10(a). "An authorization for the release of medical information . . . shall be valid if it:

> (a) Is handwritten by the person who signs it or is in a typeface no smaller than 14-point type.
>
> (b) Is clearly separate from any other language present on the same page and is executed by a signature which serves no other purpose than to execute the authorization.
>
> (c) Is signed and dated . . .
>
> (d) States the specific uses and limitations on the types of medical information to be disclosed.
>
> (e) States the name or functions of the provider of health care, health care service plan, pharmaceutical company, or contractor that may disclose the medical information.
>
> (f) States the name or functions of the persons or entities authorized to receive the medical information.
>
> (g) States the specific uses and limitations on the use of the medical information by the persons or entities authorized to receive the medical information.
>
> (h) States a specific date after which the provider of health care, health care service plan, pharmaceutical company, or contractor is no longer authorized to disclose the medical information.
>
> (i) Advises the person signing the authorization of the right to receive a copy of the authorization.

Cal. Civ. Code § 56.11.

41. Moreover, a health care provider that maintains information for purposes covered by the CMIA is liable for negligent disclosures. Cal. Civ. Code § 56.36.[5]

42. "In addition to any other remedies available at law, any individual may bring an action against any person or entity who has negligently released confidential information or records concerning them in violation of this part, for either or both of the following: [¶] (1) ... nominal damages of one thousand dollars ($1,000). To recover under this paragraph, it shall not be necessary that the Plaintiffs suffered or was threatened with actual damages. [¶] (2) The amount of actual damages, if any, sustained by the patient." *Sutter Health v. Superior Ct.*, 227 Cal. App. 4th 1546, 1551 (2014) (quoting Cal. Civ. Code § 56.36(b)).

iii. Google's Advertising and Tracking Tools Including Google Analytics

43. Google Analytics tracks what a user communicates to Defendant's website.[6]

44. Notably, transmissions only occur on webpages that contain Tracking Tools.[7] Thus, Plaintiff's and Class Member's Private Information would not have been disclosed to Google via this technology but for Defendant's decision to install the Tracking Tools on its Website.

45. In this case, Defendant employed Tracking Tools, including the Google Analytics tool, to intercept, duplicate, and re-direct Plaintiff's and Class Members' Private Information to Google.

---

[5] "Every provider of health care ... who creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall do so in a manner that preserves the confidentiality of the information contained therein. Any provider of health care ... who negligently creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall be subject to the remedies and penalties provided under subdivisions (b) and (c) of Section 56.36." (§ 56.101, subd. (a).)

[6] *Comparing Google Analytics vs Facebook Pixel*, Boltic, https://www.boltic.io/blog/google-analytics-vs-facebook-pixel#:~:text=Google%20Analytics%20is%20a%20comprehensive,time%20on%20site%2C%20and%20conversions.&text=On%20the%20other%20hand%2C%20Facebook,user%20actions%20on%20your%20website. (last visited April 9, 2025)

[7] Defendant's Google Analytics tool stores a client ID in a first-party cookie named _ga (also identified as a cid) to distinguish unique users and their sessions on your website. Analytics doesn't store the client ID when analytics storage is disabled through Consent Mode." https://support.google.com/analytics/answer/11593727?hl=en#:~:text=Google%20Analytics%20stores%20a%20client,is%20disabled%20through%20Consent%20Mode. (last visited April 9, 2025).

46. Defendant's Source Code manipulated the patient's browser by secretly instructing it to duplicate the patient's communications (HTTP Requests) with Defendant and to send those communications to Google. These transmissions occurred contemporaneously, invisibly, and without the patient's knowledge.

47. Thus, without its patients' consent, Defendant has effectively used its source code to commandeer and "bug" or "tap" it patients' computing devices, allowing Google, and other third parties to listen in on all of their communications with Defendant and thereby intercept those communications, including Private Information.

48. The Tracking Tools allow Defendant to optimize the delivery of ads, measure cross-device conversions, create custom audiences, and decrease advertising and marketing costs. However, Defendant's Website does not rely on the Tracking Tools in order to function.

49. While seeking and using Defendant's services as a medical provider, Plaintiff and Class Members communicated their Private Information to Defendant via its Website.

50. Plaintiff and Class Members were not aware that their Private Information would be shared with third parties as it was communicated to Defendant because, amongst other things, Defendant did not disclose this fact.

51. Plaintiff and Class Members never consented, agreed, authorized, or otherwise permitted Defendant to disclose their Private Information to third parties, nor did they intend for anyone other than Defendant to be a party to their communications (many of them highly sensitive and confidential) with Defendant.

52. Defendant's Tracking Tools sent non-public Private Information to third parties like Google, including but not limited to Plaintiff's and Class Members': (1) status as medical patients; (2) health conditions; (3) desired medical treatment or therapies; (4) desired locations or facilities where treatment was sought; (5) phrases and search queries (such as searches for symptoms, treatment options, or types of providers); (6) searched and selected physicians and their specialties conducted via the general search bar; and (7) other information related to their healthcare treatment and conditions.

53. Importantly, the Private Information Defendant's Tracking Tools sent to third parties included personally identifying information that allowed those third parties to connect the Private Information to a specific patient. Information sent to Google was sent alongside the Plaintiff's and Class Members' unique identifier ("_ga" or "CID") , thereby allowing individual patients' communications with Defendant, and the Private Information contained in those communications, to be linked to their unique Google accounts and therefore their identity.[8]

54. Similarly, Google users who are logged-in to their Google accounts also have an identifier that is stored in Google's logs. Google logs a user's browsing activities on non-Google websites and uses these data for serving personalized ads.

55. Defendant deprived Plaintiff and Class Members of their privacy rights when it: (1) implemented Tracking Tools that surreptitiously tracked, recorded, and disclosed Plaintiff's and other online patients' confidential communications and Private Information; (2) disclosed patients' protected information to unauthorized third parties; and (3) undertook this pattern of conduct without notifying Plaintiff or Class Members and without obtaining their express written consent.

56. By installing and implementing Google Analytics, Defendant caused Plaintiff's and Class Member's communications to be intercepted by and/or disclosed to Google and for those communications to be personally identifiable.

57. As explained below, these unlawful transmissions are initiated by Defendant's source code concurrent with communications made via certain webpages.

[8] *See Brown v. Google, Inc.*, *Brown v. Google LLC*, 525 F. Supp. 3d 1049 (N.D. Cal. 2021) (citing internal evidence from Google employees). Google also connects user data to IP addresses; IP addresses have been classified by the United States Department of Health and Human Services ("HHS") as personally identifying information. *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, U.S. Dept of Health and Hum. Servs. (Dec. 1, 2024), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.

B. BSCA Assisted Third Parties in Intercepting Patients' Communications with its Web Properties and Disclosed Plaintiff's and Class Members' Private Information to Third Parties.

58. BSCA's Web Properties are accessible on mobile devices and desktop computers and allow patients to communicate with BSCA regarding their past, present, and future health care, as well as their past, present, and future medical bills, insurance coverage, and payments.

59. BSCA encouraged patients to use the Web Properties to communicate their private information, acquire insurance, identify in-network healthcare providers based on the specific treatment or services they are interested in via the "Find a Doctor" search bar, access information about their insurance coverage, submit claims, pay bills, view records, and more.

60. Despite this, BSCA purposely installed Tracking Technologies on its Web Properties and programmed them to surreptitiously share its patients' private and protected communications, including Plaintiff's and Class Members' PHI and PII, which was sent to Google.

61. The Tracking Technologies intercepted, recorded, and disseminated patients' information as they navigated and communicated with BSCA via the Web Properties, simultaneously and invisibly transmitting the substance of those communications to unintended and undisclosed third parties.

62. The information the Tracking Technologies allowed to be sent and received by third parties constitutes Private Information and includes the following:

(a) Insurance plan name, type and group number;

(b) City and zip code;

(c) Gender and family size;

(d) Blue Shield assigned identifiers for members' online accounts;

(e) medical claim service date and service provider, patient name, and patient financial responsibility; and

(f) "Find a Doctor" search criteria and results (location, plan name and type, provider name and type).

63. The information collected and disclosed by BSCA's Tracking Tools is not anonymous and is viewed and categorized by the intercepting party on receipt.

64. The Private Information intercepted by and disclosed to Google includes identifying information that allows those third parties to know exactly whose information they have acquired.

65. For example, Google "stores users' logged-in identifier on non-Google website in its logs. Whenever a user logs-in on non-Google websites, whether in private browsing mode or non-private browsing mode, the same identifier is associated with the data Google collects from the user's browsing activities on that website. Google further logs all such data (private and non-private) within the same logs and uses these data for serving personalized ads."

66. Simply put, the Private Information that was disclosed via the Tracking Tools is personally identifiable and was sent alongside other persistent identifiers such as the patients' IP address, Google account ID, and device identifiers.[9]

67. As described by the HHS Bulletin, this is protected health information (PHI) even if the visitor has no previous relationship with BSCA because "the information connects the individual to the regulated entity (*i.e.*, it is indicative that the individual has received or will receive health care services or benefits from the covered entity), and thus relates to the individual's past, present, or future health or health care or payment for care."[10]

a. Google Received Plaintiff's and Class Members' Private Information via Tracking Technologies Installed on BSCA's Web Properties.

68. BSCA utilized Google Analytics and intentionally installed it along with Google Ads and related Google business tools on its Web Properties.

69. Google Analytics allows BSCA to optimize the delivery of ads, measure cross-device conversions, create custom audiences (for future targeted marketing and advertising), and

[9] *Id.*

[10] *See* HHS Bulletin § *How do the HIPAA Rules apply to regulated entities' use of tracking technologies?*

decrease its advertising and marketing costs. However, BSCA's Web Properties do not require Google Analytics or any other Tracking Tools to function.

70. Plaintiff and Class Members never consented, agreed, authorized, or otherwise permitted BSCA to disclose their Private Information to Google, nor did they intend for Google to be a party to their communications (many of them highly sensitive and confidential) with BSCA.

71. BSCA's Google Analytics tool sent non-public Private Information to Google, including but not limited to information about Plaintiff's and Class Members' past, present, or future health or health care and payment for past, present, or future health care. *See Supra* ¶52.

72. Importantly, the Private Information Google received was sent alongside Plaintiff's and Class Members' IP address, Google Client identifier (cid), and other persistent device identifiers.

73. As stated above, a Google Client ID (cid), as stored in the _ga cookie, is a unique identifier for a browser-device pair. It is used by Google Analytics to track user interactions across sessions on a specific website.

74. Google Analytics uses both first- and third-party cookies, and both were used on the Web Properties.[11] Notably, it is nearly impossible for website users to block first-party cookies such as the _ga cookie. Doing so requires specialized knowledge and tools, and often results in the website not functioning properly.

75. Stated differently, even individuals who take extra steps to safeguard their privacy by using ad blockers and blocking third-party cookies cannot prevent BSCA's dissemination of their information to Google.

76. BSCA used Google Analytics alongside Google Tag Manager, and related tools that communicate with Google Ad Services and DoubleClick, all of which were installed on BSCA's Web Properties. Though BSCA claims to have removed all of the Google Analytics and

[11] A first-party cookie is "created by the website the user is visiting"—in this case, Defendant's Website. A third-party cookie is "created by a website with a domain name other than the one the user is currently visiting"—i.e., Google. The _ga cookie is always transmitted as a first-party cookie.

associated Tracking Technologies, the screenshots below depict a different story. The Google Tag Manager which typically works in tandem with Google Analytics is still firing as of April 10, 2025, a day after Defendant sent out its "Data Breach Notice", which notified Plaintiff, Class Members, and existing patients that they recognized they were releasing data.

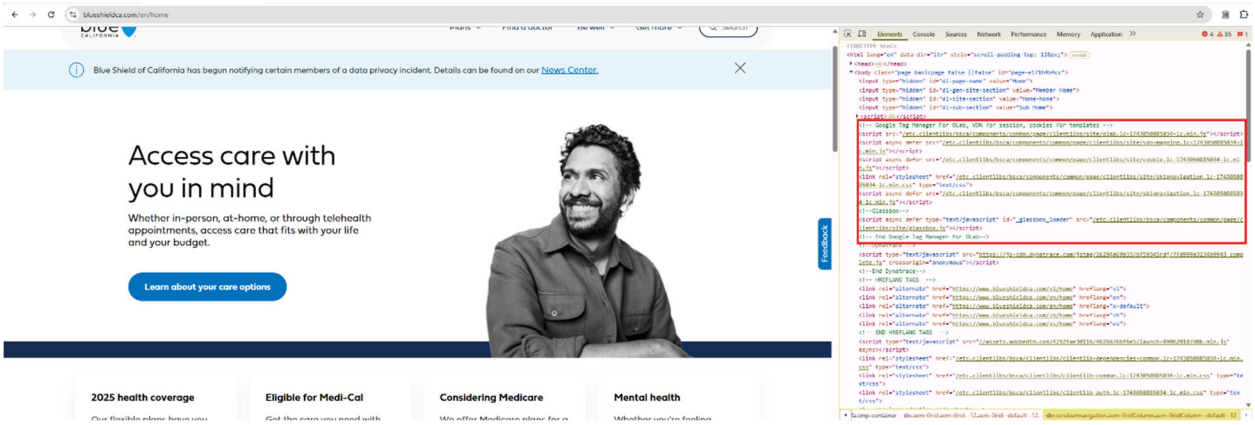

Figure 1: Screenshot of https://blueshieldca.com/en/home depicting the Google Tag Manager element still actively firing.

```
<!-- Google Tag Manager For OLab, VDN for session, cookies for templates -->
<script src="/etc.clientlibs/bsca/components/common/page/clientlibs/site/olab.lc-1743050885034-lc.min.js"></script>
<script async defer src="/etc.clientlibs/bsca/components/common/page/clientlibs/site/vdn-mapping.lc-1743050885034-lc.min.js"></script>
<script async defer src="/etc.clientlibs/bsca/components/common/page/clientlibs/site/cookie.lc-1743050885034-lc.min.js"></script>
<link rel="stylesheet" href="/etc.clientlibs/bsca/components/common/page/clientlibs/site/skipnavigation.lc-1743050885034-lc.min.css" type="text/css">
<script async defer src="/etc.clientlibs/bsca/components/common/page/clientlibs/site/skipnavigation.lc-1743050885034-lc.min.js"></script>
<!--Glassbox-->
<script async defer type="text/javascript" id="_glassbox_loader" src="/etc.clientlibs/bsca/components/common/page/clientlibs/site/glassbox.js"></script>
<!-- End Google Tag Manager For OLab-->
```

Figure 2: Zoomed in section of Figure 1 depicting Google Tag Manager element running for the users session, utilizing cookies for templates.

77. Google Tag Manager ("GTM") is a free tracking tool and management platform that allows a developer to add marketing tags, or snippets of code, to its website to track and collect marketing data. It allows developers to easily implement GTM tags without modifying the code while improving the amount and type of information gathered.[12] A developer can "[u]se Tag

[12] https://evolve-systems.com/blog/what-does-google-tag-manager-do-the-benefits-of-google-tag-manager-and-what-to-track/#:~:text=Google%20Tag%20Manager%20(GTM)%20is%20a%20free,website%20to%20track%20and%20collect%20marketing%20data. (last visited April 9, 2025)

Manager to manage tags (such as measurement and marketing optimization JavaScript tags) on your site. Without editing your site code, use Tag Manager to add and update Google Ads, Google Analytics, Floodlight, and third-party tags."[13]

78. Tags are small pieces of code that track user activity, send data to analytics platforms, or trigger specific actions on the users website.

79. While Google Analytics is the hub for analyzing website data, Google Tag Manager is the tool for transmitting the data points. GTM essentially controls what information is sent to Google Analytics in order to be analyzed. GTM is the platform for deploying and storing the tags without the capacity to examine analyzed reports, which is why the data is sent to Google Analytics. Together, Google Tag Manager and Google Analytics track and create analytics relating to a website.[14]

80. GTM facilities tracking of PDF downloads, scrolling behavior, link clicks, form submissions, video activity, and more.[15]

81. Google views, uses, and monetizes the data it receives for marketing and links Private Information to other information in its possession.

82. BSCA did not disclose that the Tracking Technologies it embedded in its Web Properties intercept, transmit, record, and disseminate Plaintiff's and Class Members' Private Information to Google or additional third parties who use Google's marketing services.

83. Moreover, BSCA never received consent or written authorization to disclose Plaintiff's and Class Members' Private Information in this manner.

[13] https://developers.google.com/tag-platform/tag-manager (last visited April 9, 2025)
[14] https://evolve-systems.com/blog/what-does-google-tag-manager-do-the-benefits-of-google-tag-manager-and-what-to-track/#:~:text=Google%20Tag%20Manager%20(GTM)%20is%20a%20free,website%20to%20track%20and%20collect%20marketing%20data. (last visited April 9, 2025)
[15] *Id.*

D. Plaintiff's and Class Members' Private Information was Viewed and Used by Unauthorized Third Parties such as Google.

84. Unsurprisingly, the Tracking Technologies are not offered for "free" to companies like Defendant solely for Defendant's benefit. "Data is the new oil of the digital economy,"[16] and Google's online advertising business generated 42.4% of global digital ad revenues in 2023.[17]

85. Thus, the large volumes of personal and sensitive health-related data Defendant divulged was viewed, examined, analyzed, curated, and used by Google.

86. Technology companies acquire the raw data to transform it into a monetizable commodity, just as an oil company acquires crude oil to transform it into gasoline. Indeed, Google offers Tracking Tools like Google Analytics free of charge, and the price that Defendant paid was the data it allowed them to intercept from Plaintiff's and Class Members' devices, and the data that it disseminated directly from BSCA's own servers.

87. Even if Google eventually deletes or anonymizes sensitive information that it receives, it must first view that information to identify it as containing sensitive information suitable for removal. Accordingly, there is a breach of confidentiality the instant the information is disclosed or received without authorization. As described by the HHS Bulletin:

> It is insufficient for a tracking technology vendor to agree to remove PHI from the information it receives or de-identify the PHI before the vendor saves the information. Any disclosure of PHI to the vendor without individuals' authorizations requires the vendor to have a signed BAA in place **and** requires that there is an applicable Privacy Rule permission for disclosure.

(emphasis in original).

E. Defendant Was Enriched and Benefitted from the Use of the Tracking Technology and Private Information Has Financial Value

88. The Tracking Technologies served the purpose of bolstering Defendant's profits via marketing and advertising.

[16] https://www.wired.com/insights/2014/07/data-new-oil-digital-economy/.

[17] https://visiblealpha.com/blog/global-digital-advertising-revenues-a-look-at-the-big-three-alphabet-googl-meta-platforms-meta-amazon-com-amzn/ (last visited April 10, 2025).

89. In exchange for bartering away and disclosing the Private Information of its patients and customers, BSCA is compensated by Google in the form of enhanced advertising services and more cost-efficient marketing.

90. Retargeting is a form of online marketing that targets users with ads based on their previous internet communications and interactions.

91. By utilizing the Tracking Technologies, the cost of advertising and retargeting was reduced, thereby benefiting Defendant.

92. BSCA's disclosure of Private Information harmed Plaintiff and the Class. Conservative estimates suggest that in 2018, Internet companies earned $202 per American user from mining and selling data. That figure is expected to continue to increase and estimates for 2022 were as high as $434 per user, constituting over $200 billion industry wide.

93. The value of health data in particular is well-known. For example, Time Magazine published an article in 2017 titled "How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry" in which it described the extensive market for health data, observing that the market for this data is both lucrative and a significant risk to privacy.[18]

94. Similarly, CNBC published an article in 2019 in which it observed that "[d]e-identified patient data has become its own small economy: There's a whole market of brokers who compile the data from providers and other health-care organizations and sell it to buyers."[19] Accordingly, patient data that can be linked to a specific individual is even more valuable.

95. There is also a market for data in which consumers can participate. Personal information has been recognized by courts as extremely valuable. *See In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 462 (D. Md. 2020) ("Neither should the Court ignore what common sense compels it to acknowledge—the value that personal identifying information has in our increasingly digital economy. Many companies, like Marriott, collect

[18] *See* https://time.com/4588104/medical-data-industry/ (last visited April 10, 2025).
[19] *See* https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html (last visited April 10, 2025).

personal information. Consumers too recognize the value of their personal information and offer it in exchange for goods and services.").

96. Several companies have products through which they pay consumers for a license to track their data. Google, Nielsen, UpVoice, HoneyGain, and SavvyConnect are all companies that pay for historical browsing information.

97. Meta also has paid users for their digital information, including browsing history. Until 2019, Meta ran a "Facebook Research" app through which it paid $20 a month for a license to collect browsing history information and other communications from consumers between the ages 13 and 35.

98. Additionally, healthcare data is extremely valuable to bad actors. Health care records may be valued at up to $250 per record on the black market.[20]

99. Personal information has private value beyond its use as a bare commodity.[21] The value of personal information is thus inherently related to the value of privacy, which is a question that has been researched in multiple fields including decision science, economics, information systems, management, health care, and marketing.[22] This research has approached the valuation of personal information from multiple perspectives:[23]

(a) The amount one would accept to relinquish their data;

(b) The amount one would spend to protect their data;

(c) The potential harm from data exposure; and

(d) The benefit a data holder could gain from acquiring data.

[20] Tori Taylor, *Hackers, Breaches, and the Value of Healthcare Data, SecureLink* (June 30, 2021), https://www.securelink.com/blog/healthcare-data-new-prize-hackers.

[21] *Wagner, et. al* (2018); Acquisti, Alessandro, Curtis Taylor, and Liad Wagman (2016); Li, Xiao-Bai, Xiaoping Liu, and Luvai Motiwalla (2021).

[22] Fehrenbach David, Carolina Herrando, "The effect of customer-perceived value when paying for a product with personal data: A real-life experimental study." *Journal of Business Research* 137 (2021): 222-232; Li, Xiao-Bai, Xiaoping Liu, and Luvai Motiwalla (2021); Alorwu, et al. (2024).

[23] Acquisti, Alessandro, Curtis Taylor, and Liad Wagman, "The Economics of Privacy," Journal of Economic Literature 54 (2): 442–92 (2016).

100. These approaches can be used to establish a set of data points for the reasonable estimation of the value of personal information and non-public medical information such as patient status.

101. In addition, numerous services exist that charge fees to monitor and remove personal information from data brokers and search databases. For example, Privacy Bee offers data removal and privacy services.[24] Other similar services exist today, such as DeleteMe, which removes information from all major data broker websites,[25] Incogni.com which removes information from major data broker websites and search databases,[26] and ReputationDefender, a service that removes personal information from various databases.[27] These provide a baseline market valuation of personal information

F. Defendant Violated HIPAA and Industry Standards.

102. In December 2022, HHS issued a bulletin (the "HHS Bulletin") warning regulated entities like Defendant about the risks presented by the use of Tracking Tools on their websites:

> Regulated entities [those to which HIPAA applies] are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules. ***For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures.***[28]

103. In other words, the HHS has expressly stated that entities who implement Tracking Tools, such as Defendant, have violated HIPAA Rules unless they have obtained a HIPAA-complaint authorization from their patients.

---

[24] Privacy Bee - Pricing, privacybee.com.
[25] Deleteme - deleteme.com.
[26] Incogni - incogni.com.
[27] ReputationDefender - me.reputationdefender.com. ReputationDefender was previously known as Reputation.com and has been offering this service since at least 2012. Also see: https://www.nytimes.com/2012/12/09/business/company-envisions-vaults-for-personal-data.html
[28] *See Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates* (Dec. 1, 2022), available at https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (last visited April 10, 2025) (emphasis added).

104. The HHS Bulletin further warns that:

> While it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors, ***because of the proliferation of tracking technologies collecting sensitive information, now more than ever, it is critical for regulated entities to ensure that they disclose PHI only as expressly permitted or required by the HIPAA Privacy Rule.*** [29]

105. In addition, HHS and the FTC have recently issued a letter, once again admonishing entities like Defendant to stop using Tracking Tools:

> If you are a covered entity or business associate ("regulated entities") under HIPAA, you must comply with the HIPAA Privacy, Security, and Breach Notification Rules (HIPAA Rules), with regard to protected health information (PHI) that is transmitted or maintained in electronic or any other form or medium. ***The HIPAA Rules apply when the information that a regulated entity collects through tracking technologies or discloses to third parties (e.g., tracking technology vendors) includes PHI. . .*** Even if you are not covered by HIPAA, you still have an obligation to protect against impermissible disclosures of personal health information under the FTC Act and the FTC Health Breach Notification Rule. . . As recent FTC enforcement actions demonstrate, it is essential to monitor data flows of health information to third parties via technologies you have integrated into your website or app. The disclosure of such information without a consumer's authorization can, in some circumstances, violate the FTC Act as well as constitute a breach of security under the FTC's Health Breach Notification Rule.[30]

106. Under Federal Law, a healthcare provider may not disclose personally identifiable, non-public medical information about a patient, a potential patient, or household member of a patient for marketing purposes without the patients' express written authorization.[31]

107. The HIPAA Privacy Rule, located at 45 CFR Part 160 and Subparts A and E of Part 164, "establishes national standards to protect individuals' medical records and other individually identifiable health information (collectively defined as 'protected health information') and applies

---

[29] *Id.*

[30] *Re: Use of Online Tracking Technologies*, U.S. Dept. of Health & Hum. Servs. and Fed. Trade. Comm'n (July 20, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf.

[31] HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502; 164.508(a)(3), 164.514(b)(2)(i).

to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically."[32]

108. The Privacy Rule broadly defines "protected health information" ("PHI") as individually identifiable health information ("IIHI") that is "transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium." 45 C.F.R. § 160.103.

109. IIHI is defined as "a subset of health information, including demographic information collected from an individual" that is: (1) "created or received by a health care provider, health plan, employer, or health care clearinghouse"; (2) "[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual"; and (3) either (a) "identifies the individual" or (b) "[w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual." 45 C.F.R. § 160.103.

110. Under the HIPAA de-identification rule, "health information is not individually identifiable only if": (1) an expert "determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information" and "documents the methods and results of the analysis that justify such determination'"; or (2) "the following identifiers of the individual or of relatives, employers, or household members of the individual are removed;

(a) Names;

(b) Medical record numbers;

(c) Account numbers;

(d) Device identifiers and serial numbers;

(e) Web Universal Resource Locators (URLs);

(f) Internet Protocol (IP) address numbers; … and

[32] HHS.gov, HIPAA For Professionals (last visited April 10, 2025), https://www.hhs.gov/hipaa/forprofessionals/privacy/index.html.

> (g) Any other unique identifying number, characteristic, or code…; and" The covered entity must not "have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information."

45 C.F.R. § 160.514.

111. The HIPAA Privacy Rule requires any "covered entity" to maintain appropriate safeguards to protect the privacy of protected health information and sets limits and conditions on the uses and disclosures that may be made of protected health information without authorization. 45 C.F.R. §§ 160.103, 164.502.

112. An individual or corporation violates the HIPAA Privacy Rule if it knowingly and in violation of 42 U.S.C. §§ 1320d-1320d-9 ("Part C"): "(1) uses or causes to be used a unique health identifier; [or] (2) obtains individually identifiable health information relating to an individual." The statute states that a "person … shall be considered to have obtained or disclosed individually identifiable health information in violation of [Part C] if the information is maintained by a covered entity … and the individual obtained or disclosed such information without authorization." 42 U.S.C. § 1320d-6.

113. The criminal and civil penalties imposed by 42 U.S.C. § 1320d-6 apply directly to Defendant when it is knowingly disclosing individually identifiable health information relating to an individual, as those terms are defined under HIPAA.

114. Violation of 42 U.S.C. § 1320d-6 is subject to criminal penalties. 42 U.S.C. § 1320d-6(b). There is a penalty enhancement where "the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm." In such cases, the entity that knowingly obtains individually identifiable health information relating to an individual shall "be fined not more than $250,000, imprisoned not more than 10 years, or both."

115. In Guidance regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act Privacy Rule, the HHS instructs:

> Identifying information alone, such as personal names, residential addresses, or phone numbers, would not necessarily be designated as PHI. For instance, if such information was reported as part of a publicly accessible data source, such as a phone book, then this information would not be PHI because it is not related to health data… If such information was listed with health condition, health care provision, or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI.[33]

116. In its guidance for Marketing, the HHS further instructs:

> The HIPAA Privacy Rule gives individuals important controls over whether and how their protected health information is used and disclosed for marketing purposes. With limited exceptions, the Rule requires an individual's written authorization before a use or disclosure of his or her protected health information can be made for marketing. … Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party's own purposes. Moreover, *covered entities may not sell lists of patients to third parties without obtaining authorization from each person on the list*. (Emphasis added).[34]

117. As alleged above, there is an HHS Bulletin that highlights the obligations of "regulated entities," which are HIPAA-covered entities and business associates, when using tracking technologies.[35]

118. The Bulletin expressly provides that "[r]egulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules."

119. Defendant's actions violated HIPAA Rules.

---

[33]https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf.

[34]https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf.

[35] *See* https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.

G. IP Addresses, Mobile Advertising IDs, and Other Devices Identifiers Constitute Personally Identifiable Information.

120. BSCA also disclosed and otherwise assisted third parties with intercepting Plaintiff's and Class Members' IP addresses, Mobile Advertising IDs, and other device identifiers that are uniquely linked to specific individuals.

121. An IP address is a number that identifies the address of a device connected to the Internet, and it is used to identify and route communications on the Internet.

122. Internet service providers, websites, and third-party tracking companies use individual's IP addresses to facilitate and track Internet communications.

123. As noted above, Defendant used Google Analytics tools, Google Tag Manager, and DoubleClick tracking tools without anonymizing users' IP addresses.

124. Under HIPAA, an IP address is considered personally identifiable information:

- HIPAA defines personally identifiable information to include "any unique identifying number, characteristic or code" and specifically lists the example of IP addresses. See 45 C.F.R. § 164.514 (2).
- HIPAA further declares information as personally identifiable where the covered entity has "actual knowledge that the information to identify an individual who is a subject of the information." 45 C.F.R. § 164.514(2)(ii); See also, 45 C.F.R. § 164.514(b)(2)(i)(O).

125. Consequently, by disclosing IP addresses, Defendant's business practices violated HIPAA and industry privacy standards.

126. Likewise, on information and belief, the Tracking Tools used by Defendant also transmitted users' Mobile Advertising IDs ("MAID") and may have transmitted AAID (Android Advertising ID), Router SSID, Hardware ID, IMEI (International Mobile Equipment Identity), and other persistent identifiers.

127. According to the FTC, "MAIDs and other persistent identifiers, by design, enable direct communication with individual consumers, are used to amass profiles of individuals over

time and across different web and mobile services, and are the basis to make decisions and insights about individual consumers."[36]

H. Plaintiff's Experience with Defendant's Web Properties

128. Plaintiff Ashley Johnson has been insured by BSCA and used BSCA's services for several years.

129. As a member of BSCA's insurance plans, and in order to obtain medical treatment and insurance services, Plaintiff accessed and used BSCA's Web Properties on her phone and computer. She has used these same devices to access her Google account and email, and she stays logged into these accounts.

130. Plaintiff Johnson communicated her Private Information to BSCA when she used the Web Properties, and she used the "Find a Doctor" form and webpage to identify a healthcare provider.

131. She used the filtering feature to obtain the narrowest selection, which communicated the following: (1) the type of physician or medical provider she was seeking; (2) the specific medical services she was seeking; (3) her location; and (4) additional details about her desired physician and their practice area.

132. Upon entering her Private Information and clicking the "Search" button, her search parameters and the contents of her communications were sent to Google alongside her IP address, Google Client ID, and additional persistent identifiers that reveal her identity.

133. Plaintiff Johnson reasonably expected that—as a health plan member seeking medical treatment and services—her Private Information and communications were confidential and would not be received by Google or other unknown third-parties, or used for marketing purposes, without her express written consent.

134. She received an email from Defendant on April 9, 2025 informing her about the privacy breach described throughout this Complaint.

[36] *See In the Matter of Gravy Analytics, Inc., a corporation, and Venntel, Inc., a corporation* (Compl. 212-3025), available online at https://www.ftc.gov/system/files/ftc_gov/pdf/2123035gravyanalyticscomplaint.pdf.

135. The risk to Plaintiff's and other patients' privacy is ongoing in nature because the Private Information Google received can be used for years to come. Additionally, a portion of Google's tracking tools are still operating on Defendant's web properties as of April 10, 2025.

136. Importantly, many companies are using data obtained by Tracking Tools to decide whether to raise insurance premiums or deny coverage.[37]

137. Through the process detailed in this Complaint, BSCA unlawfully assisted Google with intercepting Plaintiff's communications and health information via Google Analytics, breached confidentiality, violated Plaintiff's right to privacy, and unlawfully disclosed her personally identifiable information and protected health information.

138. Plaintiff was unaware that BSCA installed Tracking Tools on its Web Properties because, amongst other things, the Tracking Tools were and are completely invisible, and Plaintiff reasonably believed her health insurance provider would safeguard her privacy in compliance with industry standards, HIPAA, and relevant laws.

139. Plaintiff has a continuing interest in ensuring that future communications with Defendant are protected and safeguarded from future unauthorized disclosure and to know the precise categories of information disclosed, to whom it was disclosed, and why it was disclosed.

TOLLING

140. Any applicable statute of limitations has been tolled by the "delayed discovery" rule. Plaintiff did not know (and had no way of knowing) that her Private Information was intercepted and unlawfully disclosed to Google or any other third-parties in the manner described herein because: (1) Defendant kept this information secret, and (2) the Tracking Tools are invisible on Defendant's the Web Properties.

[37] *See In re Consumer Vehicle Driving Data Tracking Litig.*, 737 F. Supp. 3d 1355 (U.S. Jud. Pan. Mult. Lit. 2024)(alleging General Motors and OnStar improperly used Tracking Tools to disseminate information to third-parties); *see also The State of Texas v. The Allstate Corporation et al., Dist. Ct. of Tex.*, Montgomery Cty. (available online at https://www.texasattorneygeneral.gov/sites/default/files/images/press/Allstate%20and%20Arity%20Petition%20Filed.pdf).

CLASS ACTION ALLEGATIONS

141. Plaintiff brings this lawsuit under Federal Rules of Civil Procedure 23(a), (b)(1), (b)(2), and (b)(3), and/or (c)(4) on behalf of the following:

> **Nationwide Class:** United States citizens who, during the Class Period, used Defendant's Web Properties and had their personally identifiable information or protected health information disclosed to Google or other third parties as a result of using the Web Properties.
>
> **California Class:** All California residents who, during the Class Period, used Defendant's Web Properties and had their personally identifiable information or protected health information disclosed to Google or other third parties as a result of using the Web Properties.

142. Plaintiff reserves the right to modify the class definitions or add sub-classes as needed prior to filing a motion for class certification.

143. The "Class Period" is the period beginning on the date established by the Court's determination of any applicable statute of limitations, after consideration of any tolling, concealment, and accrual issues, and ending on the date of entry of judgement or preliminary approval of a settlement.

144. Excluded from the Class are Defendant; any affiliate, parent, or subsidiary of Defendant; any entity in which Defendant has a controlling interest; any officer director, or employee of Defendant; any successor or assign of Defendant; anyone employed by counsel in this action; any judge to whom this case is assigned, his or her spouse and immediate family members; and members of the judge's staff.

145. Numerosity. Members of the Class are so numerous that joinder of all members would be unfeasible and not practicable. The exact number of Class Members is unknown to Plaintiff currently. However, it is estimated that there are thousands of individuals in the Class. The identity of such membership is readily ascertainable from Defendant's records, including records of all people to whom Defendant sent the Notice of Data Breach.

146. Typicality. Plaintiff's claims are typical of the claims of the Class because Plaintiff had her personally identifiable information and protected health information disclosed to third

parties such as Google without her express written authorization or knowledge. Plaintiff's claims are based on the same legal theories as the claims of other Class Members.

147. Adequacy. Plaintiff is fully prepared to take all necessary steps to represent fairly and adequately the interests of the Class Members. Plaintiff's interests coincide with, and are not antagonistic to, those of the Class Members. Plaintiff is represented by attorneys with experience in the prosecution of class action litigation generally and in the emerging field of digital privacy litigation specifically. Plaintiff's attorneys are committed to vigorously prosecuting this action on behalf of the Class Members.

148. Common Questions of Law and Fact Predominate/Well Defined Community of Interest. Questions of law and fact common to the Class Members predominate over questions that may affect only individual Class Members because Defendant has acted on grounds generally applicable to the Class. Such generally applicable conduct is inherent in Defendant's wrongful conduct. The following questions of law and fact are common to the Class:

(a) Whether BSCA intentionally tapped the lines of internet communication between patients and their medical providers;

(b) Whether the Web Properties surreptitiously track PII, PHI, and related communications and simultaneously disclose(d) that information to Google and/or other third parties;

(c) Whether Google is a third-party eavesdropper;

(d) Whether BSCA's disclosures of PII, PHI, and related communications constitute an affirmative act of communication;

(e) Whether BSCA's conduct, which allowed third parties to view Plaintiff's and Class Members' PII and PHI, resulted in a breach of confidentiality;

(f) Whether BSCA's conduct, which allowed third parties to view Plaintiff's and Class Members' PII and PHI, resulted in a breach of confidence;

(g) Whether BSCA violated Plaintiff's and Class Members' privacy rights by using Tracking Technologies to communicate patients' Private Information to third parties;

(h) Whether BSCA's actions violated the Unfair Competition Law;

(i) Whether BSCA's actions violated Plaintiff's and Class Members' privacy rights as provided by the California Constitution;

(j) Whether BSCA violated HIPAA; and

(k) Whether Plaintiff and Class Members are entitled to damages.

149. Superiority. Class action treatment is a superior method for the fair and efficient adjudication of the controversy. Such treatment will permit many similarly situated persons to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, or expense that numerous individual actions would engender. The benefits of proceeding through the class mechanism, including providing injured persons a method for obtaining redress on claims that could not practicably be pursued individually, substantially outweighs potential difficulties in management of this class action. Plaintiff is unaware of any special difficulty to be encountered in litigating this action that would preclude its maintenance as a class action.

150. Class certification is also appropriate under Rules 23(b)(1), (b)(2), and/or (c)(4) because:

- The prosecution of separate actions by the individual members of the Class would create a risk of inconsistent or varying adjudications establishing incompatible standards of conduct for Defendant;
- The prosecution of separate actions by individual Class Members would create a risk of adjudications that would, as a practical matter, be dispositive of the interests of other Class Members not parties to the adjudications, or would substantially impair or impede their ability to protect their interests;
- Defendant has acted or refused to act on grounds generally applicable to the Class, making injunctive and corresponding declaratory relief appropriate with respect to the Class as a whole; and
- The claims of Class Members are comprised of common issues whose resolution in a class trial would materially advance this litigation,

CLAIMS FOR RELIEF

FIRST CAUSE OF ACTION
Violation Of the California Invasion of Privacy Act,
Cal. Penal Code § 631, *et seq.*
(On Behalf of Plaintiff and the California Class)

151. Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein and brings this count individually and on behalf of the proposed Class.

152. The California Invasion of Privacy Act ("CIPA") is codified at Cal. Penal Code §§ 630 to 638. The Act begins with its statement of purpose.

> The Legislature thereby declares that advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society.

Cal. Penal Code § 630.

153. California Penal Code § 631(a) provides, in pertinent part (emphasis added):

> Any person who, by means of any machine, instrument, or contrivance, or in any other manner … willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or **who aids, agrees with, employs, or conspires** with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable by a fine not exceeding two thousand five hundred dollars ($2,500).

154. Under CIPA, BSCA must show it had the consent of all parties to a communication.

155. At all relevant times, BSCA aided, employed, agreed with, and conspired with third parties, including Google, to track and intercept Plaintiff's and Class Members' internet communications. These communications were transmitted to and intercepted by a third party during the communication and without the knowledge, authorization, or consent of Plaintiff and Class Members.

156. BSCA intentionally inserted an electronic listening device onto Plaintiff's and Class Members' web browsers and devices that, without their knowledge and consent, tracked and transmitted the substance of their confidential communications to Google and other unauthorized third parties—each of whom constitute a "person" within the meaning of the statute.

157. BSCA willingly facilitated the interception and collection of Plaintiff's and Class Members' Private Information by embedding Google Analytics on its Web Properties.

158. Moreover, unlike past business tools such as the Facebook Like Button and older web beacons, Google Tag Manager, Google Analytics, and the other Tracking Tools are: (1) completely invisible to website and app users; and (2) BSCA has full control over these tools, including where they are embedded, what information is tracked and transmitted, and how events are categorized prior to their transmission.

159. BSCA's Tracking Technologies constitute "machine[s], instrument[s], or contrivance[s]" under the CIPA, and even if they do not, they fall under the broad catch-all category of "any other manner."

160. BSCA failed to disclose its use of the Tracking Technologies to specifically track and automatically and simultaneously transmit Plaintiff's and Class Members' communications to Google and other undisclosed third-parties.

161. A portion of the Tracking Technologies—such as Google Analytics and Google Tag Manager—are designed to transmit a website user's actions and communications contemporaneously as the user initiates each communication. As a result, the user's communications are intercepted in transit to the intended recipient—BSCA—before reaching BSCA's server.

162. BSCA violated CIPA by aiding and permitting third parties to intercept and receive its patients' online communications in real time as they were made. Importantly, Google and other unauthorized third parties would not have intercepted or received the contents of these communications but for BSCA's actions, including its decision to install the Tracking Tools on its Web Properties.

163. By disclosing Plaintiff's and Class Members' Private Information, BSCA violated Plaintiff's and Class Members statutorily protected right to privacy.

164. As a result of the above violations, and pursuant to CIPA Section 637.2, BSCA is liable to Plaintiff and Class Members for actual damages related to their loss of privacy in an amount to be determined at trial or for statutory damages in the amount of $5,000 per violation. Section 637.2 specifically states that "[it] is not a necessary prerequisite to an action pursuant to this section that the Plaintiffs have suffered, or be threatened with, actual damages."

165. Under the statute, BSCA is also liable for reasonable attorney's fees, litigation costs, injunctive and declaratory relief, and punitive damages in an amount to be determined by a jury, but sufficient to prevent the same or similar conduct by the Defendant in the future.

SECOND CAUSE OF ACTION
Violation of the California Invasion of Privacy Act,
Cal. Penal Code § 638.51(a)
(On behalf of Plaintiff and the California Class)

166. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein and brings this claim individually and on behalf of the proposed Class.

167. CIPA § 638.51(a) proscribes any "person" from "install[ing] or us[ing] a pen register or a trap and trace device without first obtaining a court order."

168. A "pen register" is a "device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of the communication." Cal. Penal Code § 638.50(b).

169. The Tracking Tools are "pen registers" because they are device[s] or process[es]" that "capture[d]" the "routing, addressing, or signaling information" from Plaintiffs and Class Members' electronic communications. *Id.*

170. At all relevant times, BSCA installed the Tracking Tools—which are pen registers—onto Plaintiff's and Class Members' browsers, and it used the Tracking Tools to capture Plaintiff's and Class Members' Private Information.

171. Plaintiff and Class Members did not provide their consent to BSCA's installation or use of the Tracking Tools.

172. BSCA did not obtain a court order to install or use the Tracking Tools.

173. Pursuant to Cal. Penal Code § 637.2, Plaintiff and Class Members have been injured by BSCA's violations of CIPA § 638.51(a), and each seek statutory damages of $5,000 for each of BSCA's violations of CIPA § 638.51(a).

THIRD CAUSE OF ACTION
Violation Of the California Confidentiality of Medical Information Act
Cal. Civ. Code § 56, *et seq.*
(On Behalf of Plaintiff and the California Class)

174. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein and brings this claim individually and on behalf of the proposed Class.

175. The California Confidentiality of Medical Information Act, Cal. Civ. Code § 56, *et seq* ("CMIA") prohibits health care service plans from disclosing medical information relating to their patients without a patient's express authorization. Medical information refers to "any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care… regarding a patient's medical history, mental or physical condition, or treatment." 'Individually Identifiable' means that the medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual..." Cal. Civ. Code § 56.05.

176. Defendant is a health care service plan as defined by Cal. Civ. Code § 56.05.

177. Plaintiff and Class Members are members of BSCA and, as a health care service plan, BSCA has an ongoing obligation to comply with the CMIA's requirements with respect to Plaintiff's and Class Members' confidential medical information.

178. As set forth above, Private Information that can uniquely identify Plaintiff and Class Members is transmitted to Google in combination with medical conditions, medical concerns, treatment(s) sought by the patients, and other patient searches and queries. This PHI and PII constitutes confidential information under the CMIA.

179. Pursuant to the CMIA, the information communicated to BSCA and disclosed to Google and other third parties constitute medical information because it is information derived from a health care service plan member regarding a patient's medical treatment and physical condition and is received in combination with individually identifying information. Cal. Civ. Code § 56.05(g) and 56.05(j).

180. As set forth above, Google views, processes, and analyzes the confidential medical information it receives via Google Analytics. Google then uses the viewed confidential information for advertising and marketing purposes.

181. Defendant failed to obtain Plaintiff's and Class Members' authorization for the disclosure of medical information.

182. Pursuant to CMIA Section 56.11, a valid authorization for disclosure of medical information must: (1) be "clearly separate from any other language present on the same page and … executed by a signature which serves no other purpose than to execute the authorization;" (2) be signed and dated by the patient or their representative; (3) state the name and function of the third party that receives the information; and (4) state a specific date after which the authorization expires. The information set forth on BSCA's Web Properties, including the website's Privacy Policy and Notice of Privacy Practices, does not qualify as a valid disclosure or authorization.

183. Defendant violated the CMIA by disclosing its patients' medical information to Google along with the patients' individually identifying information.

184. In violation of Civil Code section 56.10(e), Defendant disclosed Plaintiff's and Class members' medical information to unauthorized persons.

185. In violation of Civil Code section 56.101(b)(1)(A), Defendants' electronic health record system or electronic medical record system failed to protect and preserve the integrity of electronic medical information.

186. Defendant also violated Civil Code section 56.36(b) by negligently releasing Plaintiff's and Class members' Private Information.

187. Plaintiff and Class Members seek nominal damages, compensatory damages, punitive damages, attorneys' fees, and costs of litigation for Defendant's violations of the CMIA.

FOURTH CAUSE OF ACTION
Violation of the Unfair Competition Law
(Cal. Bus. & Prof. Code § 17200, *et seq.*)
(On Behalf of Plaintiff and the California Class)

188. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein and brings this claim individually and on behalf of the proposed Class.

189. California's Unfair Competition Law ("UCL") prohibits any "unlawful, unfair, or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising." Cal. Bus. & Prof. Code § 17200.

190. BSCA engaged in unlawful business practices in connection with its disclosure of Plaintiff's and Class Members' Private Information to unauthorized third parties, including Google, in violation of the UCL.

191. BSCA's acts, omissions, and conduct, as alleged herein, constitute "business practices" within the meaning of the UCL.

192. BSCA violated the "unlawful" prong of the UCL by violating, *inter alia*, Plaintiff's and Class Members' constitutional rights to privacy and state and federal privacy statutes, including CIPA, CMIA, and ECPA.

193. BSCA's acts, omissions, and conduct also violate the unfair prong of the UCL because those acts, omissions, and conduct offend public policy (including the federal and state privacy statutes and state consumer protection statutes, such as the ECPA, CIPA, CMIA, and HIPAA) and constitute immoral, unethical, oppressive, and unscrupulous activities that caused substantial injury to Plaintiff and Class Members.

194. The harm caused by BSCA's conduct outweighs any potential benefits attributable to such conduct, and there were reasonably available alternatives to further BSCA's legitimate business interests other than BSCA's conduct described herein, such as not using the Tracking Tools.

195. Plaintiff and Class Members suffered from a loss of the benefit of their bargain with BSCA because they overpaid for insurance services they believed included data security sufficient to maintain their Private Information as confidential.

196. As a result of BSCA's violations of the UCL, Plaintiff and Class Members are entitled to injunctive relief. This is particularly true since the dissemination of Plaintiff and Class Members' information is ongoing.

197. As a result of BSCA's violations of the UCL, Plaintiff and Class Members have suffered injury in fact and lost money or property, including but not limited to payments to BSCA for services and/or other valuable consideration, *e.g.*, access to their private and personal data.

198. Plaintiff and Class Members would not have used BSCA's services, or would have paid less for them, had they known BSCA was breaching confidentiality and disclosing their Private Information to social media and tech giants such as Google.

199. The unauthorized access to Plaintiff's and Class Members' Private Information has also diminished the value of that information.

200. In the alternative to those claims seeking remedies at law, Plaintiff and Class Members allege that there is no plain, adequate, and complete remedy that exists at law to address BSCA's unlawful and unfair business practices.

201. Further, no private legal remedy exists under HIPAA. Therefore, Plaintiff and Class Members are entitled to equitable relief to restore Plaintiffs and Class Members to the position they would have been in had BSCA not engaged in unfair competition, including an order enjoining BSCA's wrongful conduct, restitution, and disgorgement of all profits paid to BSCA as a result of its unlawful and unfair practices.

FIFTH CAUSE OF ACTION
Invasion of Privacy Under California's Constitution
(On Behalf of Plaintiff and the California Class)

202. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein and brings this claim individually and on behalf of the proposed Class.

203. Plaintiff and Class Members have an interest in: (1) precluding the dissemination and/or misuse of their Private Information; and (2) making personal decisions and/or conducting personal activities without observation, intrusion or interference, including, but not limited to, the right to visit and interact with various internet sites for the provision of insurance and health care

without being subjected to wiretaps, pin registers, and/or trap and trace devices without their knowledge or consent.

204. By using Google Analytics and accompanying Tracking Technologies to communicate patients' individually identifying information alongside their confidential medical communications and insurance information, BSCA intentionally invaded Plaintiff's and Class Members' privacy rights under the California Constitution.

205. Plaintiff and Class Members had a reasonable expectation that their communications, identity, health information and other data would remain confidential, and that BSCA would not install wiretaps, pin registers, and/or trap and trace devices to secretly transmit their communications and routing information.

206. Plaintiff and Class Members did not authorize BSCA to transmit their Private Information to third parties, nor did they consent to allowing third parties to intercept, receive, and view those communications.

207. This invasion of privacy is serious in nature, scope, and impact because it relates to patients' private medical communications. Moreover, it constitutes an egregious breach of the societal norms underlying the right of privacy.

208. As a result of BSCA's actions, Plaintiff and Class Members have suffered harm and injury, including but not limited to an invasion of their privacy rights.

209. Plaintiff and Class Members have been damaged as a direct and proximate result of BSCA's invasion of their privacy and are entitled to just compensation, including monetary damages.

210. Plaintiff and Class Members seek appropriate relief for this injury, including but not limited to damages that will reasonably compensate them for the harm to their privacy interests.

211. Plaintiff and Class Members are also seek punitive damages resulting from the malicious, willful, and intentional nature of BSCA's actions, directed at injuring Plaintiff and Class Members in conscious disregard of their rights.

212. Such damages are needed to deter BSCA from engaging in such conduct in the future.

213. Plaintiff also seeks such other relief as the Court may deem just and proper.

SIXTH CAUSE OF ACTION
Violation of the Electronic Communications Privacy Act
18 U.S.C. § 2510, *et seq*.
(On Behalf of Plaintiff and the Nationwide Class)

214. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein and brings this claim individually and on behalf of the proposed Class.

215. The Federal Wiretap Act ("FWA"), as amended by the Electronic Communications Privacy Act of 1986 ("ECPA"), prohibits the intentional interception, use, or disclosure of any wire, oral, or electronic communication.

216. In relevant part, the ECPA prohibits any person from intentionally intercepting, endeavoring to intercept, or procuring "any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication." 18 U.S.C. § 2511(1)(a).

217. The ECPA protects both sending and receipt of communications.

218. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire or electronic communications are intercepted, disclosed, or intentionally used in violation of Chapter 119.

219. The transmissions of Plaintiff's Private Information via BSCA's Web Properties qualifies as a "communication" under the ECPA's definition in 18 U.S.C. § 2510(12).

220. **Electronic Communications**. The transmission of Private Information between Plaintiff and Class Members and BSCA via its Web Properties are "transfer[s] of signs, signals, writing,…data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate commerce" and are therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(2).

221. **Content.** The ECPA defines content, when used with respect to electronic communications, to "include[] *any* information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8) (emphasis added).

222. **Interception.** The ECPA defines the interception as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or

other device" and "contents … include any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(4), (8).

223. **Electronic, Mechanical, or Other Device**. The ECPA defines "electronic, mechanical, or other device" as "any device … which can be used to intercept a[n] … electronic communication[.]" 18 U.S.C. § 2510(5). The following constitute "devices" within the meaning of 18 U.S.C. § 2510(5):

(a) Plaintiff's and Class Members' browsers;

(b) Plaintiff's and Class Members' computing devices and mobile devices;

(c) BSCA's web-servers; and

(d) The Tracking Tools deployed by BSCA to effectuate the sending and acquisition of patient communications

224. When Plaintiff and Class Members interacted with BSCA's Web Properties, BSCA, through the Tracking Tools embedded and operating on its Web Properties, contemporaneously and intentionally disclosed, used, and redirected, and endeavored to disclose, use, and redirect, the contents of Plaintiff's and Class Members' electronic communications to third parties, including Google, without authorization or consent, and knowing or having reason to know that the electronic communications were obtained in violation of the ECPA. 18 U.S.C. § 2511(1)(c)-(d).

225. BSCA's intercepted communications include, but are not limited to, the contents of communications to/from Plaintiff and Class Members regarding PII and PHI.

226. By intentionally disclosing or endeavoring to disclose the electronic communications of Plaintiff and Class Members to third parties while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), BSCA violated 18 U.S.C. § 2511(1)(c)-(d).

227. BSCA intentionally used the wire or electronic communications to increase its profit margins, and it specifically used the Tracking Tools to track and utilize Plaintiff's and Class Members' PII and PHI for financial gain.

228. BSCA was not acting under color of law to intercept Plaintiff's and Class Members' wire or electronic communication.

229. Plaintiff and Class Members did not authorize BSCA to acquire the content(s) of their communications via the Tracking Tools.

230. Any purported consent BSCA received from Plaintiff and Class Members was not valid.

231. **Unauthorized Purpose**. BSCA intentionally intercepted the contents of Plaintiff's and Class Members' electronic communications for the purpose of committing a tortious or criminal act in violation of the Constitution or laws of the United States or of any State – namely, violations of HIPAA, breaches of confidence, invasion of privacy, and violations of state privacy laws.

232. The ECPA provides that a "party to the communication" may be liable where a "communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State." 18 U.S.C § 2511(2)(d).

233. BSCA is a "party to the communication" with respect to Plaintiff's and Class Members' communications, but its simultaneous, unknown duplication, forwarding, and interception of Plaintiff's and Class Members' Private Information does not qualify for the party exemption.

234. More specifically, BSCA's acquisition of Plaintiff's and Class Members' communications, which were used and disclosed to unauthorized third parties, was done for the purpose of committing criminal and tortious acts in violation of the laws of the United States and California, including:

a) 42 U.S.C. § 1320d-6;

b) 45 CFR § 164.508(a)(1);

c) 15 U.S.C. § 45;

d) Cal. Penal Code § 631, *et seq*.;

e) Cal. Penal Code §638.51(a);

f) Cal. Civ. Code § 56, *et seq.*;

g) Cal. Bus. & Prof. Code § 17200; and

h) The common law causes of action alleged herein.

235. Under 42 U.S.C. § 1320d-6, it is a criminal violation for a person to "use[] or cause[] to be used a unique health identifier" or to "disclose[] individually identifiable health information to another person … without authorization" from the patient.

236. The penalty for violation is enhanced where "the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm." 42 U.S.C. § 1320d-6.

237. BSCA's conduct violated 42 U.S.C. § 1320d-6 in that it:

(a) Used and caused to be used persistent identifiers associated with specific patients without patient authorization; and

(b) Disclosed individually identifiable health information to Google and other unauthorized parties without patient authorization.

238. BSCA's conduct would be subject to the enhanced provisions of 42 U.S.C. § 1320d-6 because BSCA's use of the Tracking Technology was for its commercial advantage to increase revenue from existing patients and gain new patients.

239. BSCA is not exempt from ECPA liability under 18 U.S.C. § 2511(2)(d) on the ground that it was a participant in Plaintiff's and Class Members' communications because BSCA used its participation in these communications to improperly share Private Information with third-parties that did not participate in these communications (e.g., Google) when Plaintiff and Class Members: (1) were unaware those third parties would receive their Private Information; and (2) did not consent to them receiving their Private Information.

240. BSCA accessed, obtained, and disclosed Plaintiff's and Class Members' Private Information for the purpose of committing the crimes and torts described herein because it would not have been able to obtain the information or the marketing services if it had complied with the law.

241. As such, BSCA cannot viably claim any exception to ECPA liability.

242. Plaintiff and Class Members have suffered damages as a direct and proximate result of BSCA's invasion of privacy.

243. As a result of BSCA's violation of the ECPA, Plaintiff and Class Members are entitled to all damages available under 18 U.S.C. § 2520, including statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000, equitable or declaratory relief, compensatory and punitive damages, and attorney's fees and costs.

SEVENTH CAUSE OF ACTION
Common Law Invasion of Privacy – Intrusion Upon Seclusion
(On Behalf of Plaintiff and the Nationwide Class)

244. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein and brings this claim individually and on behalf of the proposed Class.

245. Plaintiff and Class Members had a reasonable expectation of privacy in their communications with BSCA via its Web Properties.

246. Plaintiff and Class Members communicated sensitive and protected medical information and individually identifiable information that they intended for only BSCA to receive and which they understood BSCA would keep private as their insurance provider and healthcare provider.

247. BSCA's disclosure of the substance and nature of Plaintiff's and Class Members' communications to third parties without their knowledge and consent is an intentional intrusion on Plaintiff's and Class Members' solitude or seclusion.

248. Plaintiff and Class Members had a reasonable expectation that their communications, identity, health information and other data would remain confidential, and that BSCA would not install: (1) wiretaps to secretly transmit their communications to unauthorized third parties; or (2) pin registers and/or trap and trace devices.

249. BSCA was authorized to receive Plaintiff's and Class Members' Private Information, but it was not authorized to commandeer Plaintiff's and Class Members' web browsers and devices, thereby forcing those devices to transmit information to Google without their consent or authorization.

250. As such, BSCA obtained Plaintiff's and Class Members' Private Information under false pretenses and/or exceeded its authority to obtain the Private Information.

251. As a result of Defendant's actions, Plaintiff and Class Members have suffered harm and injury, including but not limited to an invasion of their privacy rights.

252. Plaintiff and Class Members have been damaged as a direct and proximate result of BSCA's invasion of their privacy and are entitled to just compensation, including monetary damages.

253. Plaintiff and Class Members seek appropriate relief for that injury, including but not limited to damages that will reasonably compensate Plaintiff and Class Members for the harm to their privacy interests.

254. Plaintiff and Class Members also seek punitive damages resulting from the malicious, willful, and intentional nature of BSCA's actions, directed at injuring Plaintiff and Class Members in conscious disregard of their rights. Such damages are needed to deter BSCA from engaging in such conduct in the future.

255. Plaintiff also seeks such other relief as the Court may deem just and proper.

EIGTH CAUSE OF ACTION

Common Law Invasion of Privacy – Publication of Private Facts
(On Behalf of Plaintiff and the Nationwide Class)

256. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein and brings this claim individually and on behalf of the proposed Class.

257. Plaintiff's and Class Members' Private Information, including their communications and sensitive data, are private facts that third parties acquired without the knowledge or consent of Plaintiff and Class Members.

258. Defendant gave publicity to Plaintiff's and Class Members' Private Information and the content of their communications by sharing them with unauthorized third parties, including Google, which builds massive databases of individual consumer profiles from which to sell targeted advertising and make further disseminations.

259. Plaintiff and Class Members did not know that BSCA was using software to track and disclose their Private Information.

260. BSCA's surreptitious tracking and commoditization of Plaintiff's and Class Members' Private Information is highly offensive to a reasonable person, particularly given that BSCA provides health insurance and partners with healthcare providers to offer medical services.

261. In disseminating Plaintiff's and Class Members' personal information without their consent, BSCA acted with oppression, fraud, or malice.

262. Plaintiff and Class Members have been damaged by the publication of their Private Information and seek just compensation in the form of actual damages, general damages, unjust enrichment, nominal damages, and punitive damages.

NINTH CAUSE OF ACTION
Common Law– Breach of Confidence

263. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein and brings this claim individually and on behalf of the proposed Class.

264. Plaintiff and Class Members disclosed their Private Information in confidence to BSCA through BSCA's Web Properties.

265. Plaintiff and Class Members have an interest in keeping their protected private and medical information confidential.

266. The information disclosed in confidence is protected health and private information the Defendant had knowledge was confidential due to Federal and State laws that protect such information (i.e., HIPAA, CMIA).

267. Plaintiff and Class Members had an expectation that the confidential information disclosed to Defendant would be kept in confidence with Defendant due to their relationship with Defendant as a health services provider and Federal and State laws that protect such information (e.g., CMIA, and HIPAA).

268. BSCA violated its duty to protect the confidentiality of Plaintiff's and Class Members' information by using Tracking Tools to communicate patients' Private Information with unauthorized third parties.

269. BSCA disclosed Plaintiff's and Class Members' confidential information for BSCA's own economic benefit in BSCA's own business and disclosed it without Plaintiff's and Class Members' consent.

270. BSCA disclosed and disseminated Plaintiff's and Class Members confidential communications to a broad audience including Google and others.

271. At no time did BSCA offer to purchase or financially compensate Plaintiff and Class Members for the use of their confidential information for BSCA's advertising purposes.

272. As a result of BSCA's actions, Plaintiff and Class Members suffered harm and injury, including but not limited to a breach of their confidence, were damaged as a direct and proximate result of BSCA's breach, and seek just compensation, including monetary damages.

273. Plaintiff also seeks such other relief as the Court may deem just and proper

RELIEF REQUESTED

Plaintiff, on behalf of herself and the proposed Class, respectfully requests that the Court grant the following relief:

(a) Certification of this action as a class action and appointment of Plaintiff and Plaintiff's counsel to represent the Class;

(b) A declaratory judgement that Defendant violated: (1) the Electronic Communications Privacy Act; (2) the California Invasion of Privacy Act; (3) the California Confidentiality of Medical Information Act; (4) the Unfair Competition Law; (5) Plaintiff's and Class Members' privacy rights as provided at common law and pursuant to the California Constitution; and (6) Plaintiff's and Class Members' other rights under common law;

(c) An order enjoining BSCA from engaging in the unlawful practices and illegal acts described herein; and

(d) An order awarding Plaintiff and the Class: (1) actual, statutory, and/or nominal damages; (2) punitive damages—as warranted—in an amount to be determined at trial; (3) prejudgment interest on all amounts awarded; (4) injunctive relief as the Court may deem proper; (5) reasonable attorneys' fees and expenses and costs of suit pursuant to Cal. Code of Civil

Procedure § 1021.5 and/or other applicable law; (6) pre-judgment and post-judgment interest as provided by law; and (7) such other and further relief as the Court may deem appropriate.

DEMAND FOR JURY TRIAL

Plaintiff, individually and on behalf of the proposed Class, demands a trial by jury for all the claims asserted in this Complaint so triable.

Dated: April 10, 2025

Respectfully submitted,

/s/ Simon S. Grille

Dena C. Sharp (SBN 245869)
dsharp@girardsharp.com
Adam E. Polk (SBN 273000)
apolk@girardsharp.com
Simon S. Grille (SBN 294914)
sgrille@girardsharp.com
Isabel Velez (SBN 359574)
ivelez@girardsharp.com
GIRARD SHARP LLP
601 California Street, Suite 1400
San Francisco, CA 94108
Telephone: (415) 981-4800
Facsimile: (415) 981-4846

Counsel for Plaintiff and the Putative Class